CLAIMS AS AMENDED

1. (Amended) A method of administration of private keys for a plurality of users for use to encrypt or decrypt items transmitted via a network, there being for each user a respective set of an ID, user identifying information, private key, and public key corresponding to the private key, said method comprising:

receiving via the network a user's ID;

reading from a storage means data corresponding to the user having the received ID, which data comprises the user's private key encrypted using a key determined from identifying information of the user;

sending via the network the encrypted private key, whereby the encrypted private key can be received and decrypted at the location of the user using the user's identifying information;

receiving a digital signature manifesting the user's approval of a document, which digital signature represents a computed hash of the approved document encrypted using the user's private key; and

verifying the received digital signature by decrypting the digital signature using the user's public key and comparing the result of this decrypting with an independently computed hash of the document.

2. The method of Claim 1, wherein the user identifying information comprises a passphrase entered by the user at the user equipment, or biometric information which is obtained from the user by suitable measurement or scanning at the user equipment.

5. A method for obtaining and using a private key at user equipment via a network, said method comprising:

transmitting from the user equipment an ID of a user;

receiving a private key of the user encrypted with a user identifying key associated with the user; and

decrypting the encrypted private key using a user identifying key determined from interaction with the user at the user equipment;

using the decrypted private key; and

destroying or avoiding making any non-volatile record of the private key at the location of the user.

6. The method of Claim 5, wherein

the user identifying key determined by interaction with the user at the user equipment is determined from a passphrase entered by the user at the user equipment or biometric information which is obtained from the user by suitable measurement or scanning at the user equipment.

7. A method as claimed in Claim 5, wherein the decrypted private key is used by:

computing a hash of a document to manifest the user's approval of the document;

encrypting the hash using the user's private key; and

transmitting the encrypted hash.

8. A method as claimed in Claim 6, wherein the decrypted private key is used by:

computing a hash of a document to manifest the user's approval of the document;

encrypting the hash using the user's private key; and

transmitting the encrypted hash.

11. (Twice Amended) A system for administering private keys and corresponding public keys for a plurality of users, comprising:

computer readable storage means and

a server,

characterized in that:

the storage means includes therein respective IDs and encrypted private keys for the respective users which private keys have been encrypted using respective keys determined from respective user identifying information, and

the server is configured:

to read an encrypted private key from the storage means associated with an ID corresponding to a particular user,

to transmit the encrypted private key to the particular user,

to receive a digital signature manifesting the user's approval of a document, which digital signature represents a computed hash of the approved document encrypted using the user's private key, and

to verify the received digital signature by decrypting the digital signature using the user's public key and comparing the result of this decrypting with an independently computed hash of the document.

12. The system of Claim 11, wherein the user identifying information comprises a passphrase or biometric information.

13. (Amended) A system as claimed in Claim 11, characterized in that there is further stored in the storage means the respective public keys corresponding to the private keys for the respective users.

14. (Amended) A system as claimed in Claim 12, characterized in that there is further stored in the storage means the respective public keys corresponding to the private keys for the respective users.

15. (Twice Amended) A system as claimed in Claim 11, characterized in that

the server is further configured

to decrypt data received from the particular user using the public key.

16. (Twice Amended) A system as claimed in Claim 12, characterized in that

the server is further configured

to decrypt data received from the particular user using the public key.

19. A system as claimed in Claim 16, further comprising

at least one user terminal interconnected via a network to the server,

characterized in that the user terminal is configured

for transmitting to the server via the network an ID entered by the user, and

for receiving and decrypting an encrypted private key received via the network from the server using a user identifying key determined from a passphrase entered by the user or biometric information obtained by measuring the user.

20. A system as claimed in Claim 18, further comprising

at least one user terminal interconnected via a network to the server,

characterized in that the user terminal is configured

for transmitting to the server via the network an ID entered by the user, and

for receiving and decrypting an encrypted private key received via the network from the server using a user identifying key determined from a passphrase entered by the user or biometric information obtained by measuring the user.